OFFICE OF INSPECTOR GENERAL
UNITED STATES POSTAL SERVICE

HIGHLIGHTS

April 24, 2014

Wireless Local Area Network Deployment and Security Practices

Report Number IT-AR-14-005

BACKGROUND:

The U.S. Postal Service is committed to providing a high quality, secure, and cost-effective telecommunication infrastructure that includes a wireless local area network. This network helps link about 32,000 facilities and enable communication among hundreds of thousands of employees and systems. The Postal Service is expanding its wireless infrastructure to provide mobile connectivity in delivery units to support new applications and enhance its competitiveness in the package delivery business.

Wireless technology offers multiple benefits such as increased mobility and ease of use; however, wireless networks are easy to compromise if improperly installed, increasing the risk that the confidentiality, integrity, and availability of information systems and data will be compromised. Attackers who gain unauthorized access to wireless networks can obtain sensitive information, conduct fraudulent activities, harm networks and systems, and disrupt operations.

Our objectives were to determine whether the Postal Service has effective security policies and controls in place to detect unauthorized use of and access to its wireless network, and whether the expansion plans for its wireless infrastructure follow established policy and security standards. The vice president, Information Technology, requested this audit.

WHAT THE OIG FOUND:

We determined the Postal Service implemented adequate security policies and controls that effectively detect unauthorized use of and access to its wireless network. Specifically, the Postal Service has configured its wireless controller devices and access points to continuously monitor and detect unauthorized access.

Our wireless network discovery scans at all five facilities we reviewed did not identify any wireless access points that we considered a threat to the network, such as those installed without the network administrator's consent.

In addition, the current expansion plans for the wireless infrastructure follow established policy and security standards, and security procedures in place are effective to ensure new wireless technologies are authorized, evaluated, and assessed prior to deployment.

WHAT THE OIG RECOMMENDED:

Because the Postal Service has effective security policies and controls for managing its wireless network infrastructure and technology, we are not making any recommendations.